日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　５月１８日
出願番号 Application Number:	特願２００４－１４７４２２
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１４７４２２
出願人 Applicant(s):	松下電器産業株式会社

２００５年　５月２０日

特許庁長官
Commissioner,
Japan Patent Office

小川

【書類名】　特許願
【整理番号】　2047960086
【提出日】　平成16年 5月18日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　張　毅波
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
第１の通信装置と第２の通信装置との間で認証処理を行った上で前記第１の通信装置と前記第２の通信装置との間で通信を行う通信方法であって、
前記第２の通信装置の公開鍵情報と、前記第２の通信装置を特定するためのＩＤ情報とを含む認証要求メッセージを前記第１の通信装置に送信する認証要求ステップと、
前記第１の通信装置が受信した前記認証要求メッセージに含まれる、前記第２の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを受信した際の通信路を特定する情報とを表示する第１の表示ステップと、
前記第２の通信装置が送信した前記認証要求メッセージに含まれる、前記第２の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示する第２の表示ステップと、
前記第１の表示ステップと、前記第２の表示ステップで表示された前記第２の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第１の確認ステップと、
前記第１の確認ステップにおいて、前記第２の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第１の通信装置の公開鍵情報と、前記第１の通信装置を特定するためのＩＤ情報とを含む認証応答メッセージを前記第２の通信装置に送信する認証応答ステップと、
前記第２の通信装置が受信した前記認証応答メッセージに含まれる、前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第３の表示ステップと、
前記第１の通信装置が送信した前記認証応答メッセージに含まれる、前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第４の表示ステップと、
前記第３の表示ステップと、前記第４の表示ステップで表示された前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第２の確認ステップ
とで構成されることを特徴とする通信方法。
【請求項２】
前記認証要求ステップにおいて、認証要求メッセージはデジタル署名情報を更に含み、
前記第１の表示ステップにおいて、前記認証要求メッセージに含まれるデジタル署名情報を復号した結果、前記第２の通信装置の署名であると確認した場合に、前記第２の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示し、
前記認証応答ステップにおいて、認証応答メッセージはデジタル署名情報を更に含み、
前記第３の表示ステップにおいて、前記認証応答メッセージに含まれるデジタル署名情報を復号した結果、前記第１の通信装置の署名であると確認した場合に、前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する
ことを特徴とする請求項１記載の通信方法。
【請求項３】
前記認証要求メッセージを送信する際の通信路を特定する情報及び、前記認証応答メッセージを送信する際の通信路を特定する情報は、伝送に使用された無線チャネル情報である
ことを特徴とする請求項１または２記載の通信方法。
【請求項４】
前記認証要求メッセージを送信する際の通信路を特定する情報は、前記第２の通信装置の公開鍵情報であり、
前記認証応答メッセージを送信する際の通信路を特定する情報は、前記第１の通信装置

の公開鍵情報である
ことを特徴とする請求項１または２記載の通信方法。
【請求項５】
前記認証応答ステップにおいて、前記認証応答メッセージを前記第２の通信装置の公開鍵情報で暗号化する
ことを特徴とする請求項１または２記載の通信方法。
【請求項６】
前記第１の通信装置を特定するためのＩＤ情報及び前記第２の通信装置を特定するためのＩＤ情報は、通信路設定を行うたびに都度生成する乱数である
ことを特徴とする請求項１または２記載の通信方法。
【請求項７】
前記第２の確認ステップにおいて、前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第２の通信装置が、自身の生成した乱数を含む共通秘密鍵生成要求メッセージを前記第１の通信装置に送信する共通秘密鍵生成要求ステップと、
前記共通秘密鍵生成要求メッセージを受信した前記第１の通信装置が、自身の生成した乱数を含む共通秘密鍵生成応答メッセージを前記第２の通信装置に送信する共通秘密鍵生成応答ステップと、
前記第１の通信装置が、前記共通秘密鍵生成要求メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成し、前記第２の通信装置が、前記共通秘密鍵生成応答メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成ステップ
を更に含むことを特徴とする請求項１または２記載の通信方法。
【請求項８】
相手通信装置との間で認証処理を行った上で前記相手通信装置との間で通信を行う通信装置であって、
自装置の公開鍵及びプライベート鍵ペアを作成する公開鍵・プライベート鍵生成手段と、
前記公開鍵・プライベート鍵作成手段が生成した公開鍵情報と、自装置を識別するためのＩＤ情報とを少なくとも含む送信メッセージを生成し、前記相手通信装置に送信する送信手段と、
前記相手通信装置が送信した送信メッセージを受信し、前記相手通信装置が送信した送信メッセージに含まれる前記相手通信装置の公開鍵情報と、前記相手通信装置を識別するためのＩＤ情報とを取り出す受信手段と、
自装置が前記相手通信装置から送信メッセージを受信した場合、前記受信手段が取り出した前記相手通信装置を識別するためのＩＤ情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する機能と、自装置が前記相手通信装置に送信メッセージを送信した場合、自装置が送信した送信メッセージに含まれる、自装置を特定するためのＩＤ情報と、前記送信手段が送信メッセージを送信する際の通信路を特定する情報とを表示する機能とを有する表示手段と、
認証を許可するかとうかを入力する入力手段
とを有することを特徴とする通信装置。
【請求項９】
入力されたデータを暗号化し、その結果をデジタル署名として出力するデジタル署名手段と、
前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを暗号化する暗号化手段と、
前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを復号化する復号化手段と、

入力されたデータに対して一方向ハッシュ関数を実行するハッシュ関数手段を更に有し、
前記送信手段は、前記デジタル署名を更に含む送信メッセージを生成し、
前記受信手段は、前記受信メッセージに含まれる前記相手通信装置のデジタル署名を更に取り出し、
前記表示手段は、前記相手通信装置のデジタル署名を復号し、前記ハッシュ関数手段でハッシュ関数を実行してメッセージの正当性を確認できた場合に、前記受信手段が取り出した前記相手通信装置を識別するためのＩＤ情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する
ことを特徴とする請求項８記載の通信装置。
【請求項１０】
前記通信路を特定する情報は、伝送に使用された無線チャネル情報である
ことを特徴とする請求項８または９記載の通信装置。
【請求項１１】
前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報は、前記相手通信装置の公開鍵情報であり、
前記送信手段が送信メッセージを送信する際の通信路を特定する情報は、自装置の公開鍵情報である
ことを特徴とする請求項８または９記載の通信装置。
【請求項１２】
前記送信手段は、前記暗号化手段によって前記相手通信装置の公開鍵を使用して暗号化された送信メッセージを送信する
ことを特徴とする請求項８または９記載の通信装置。
【請求項１３】
乱数を発生させる擬似乱数発生手段を更に有し、
前記送信手段は、前記自装置を識別するためのＩＤ情報として前記擬似乱数発生手段で生成した乱数を使用する
ことを特徴とする請求項８または９記載の通信装置。
【請求項１４】
入力されたデータを用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成手段を更に有し、
前記共通秘密鍵生成手段は、前記相手通信装置が送信した送信メッセージに含まれる乱数を用いて、前記共通秘密鍵を生成する
ことを特徴とする請求項８または９記載の通信装置。

【書類名】明細書
【発明の名称】通信方法及び通信装置
【技術分野】
【０００１】
本発明は無線ＬＡＮの接続における第三者装置の不正侵入と攻撃を防ぐのに適した認証と鍵生成の方法及び装置に関するものである。
【背景技術】
【０００２】
無線ＬＡＮ接続においては、有線ＬＡＮのように繋ぐだけで接続完了となることではなく、セキュリティに関する設定も必須な項目である。無線ＬＡＮ接続のセキュリティ規格であるＩＥＥＥ　Ｓｔｄ　８０２．１１ｉでは、認証と鍵生成という二つの部分からなる接続処理が規定されており、クライアントと認証サーバまたはアクセスポイント（Ａｃｃｅｓｓ　Ｐｏｉｎｔ）が予め認証用の共通情報をもっていることが前提となる。しかし、こうした共通情報を設定するのは一般のユーザにとっては複雑で難しい。また、認証サーバを設置・設定するとすればユーザにとって非常に手間がかかる。
【０００３】
ＩＥＥＥ　Ｓｔｄ　８０２．１１ｉでは、認証の基本手順を定義しているが、それを認証サーバが普段設置されていない家庭内のネットワークを適用すると、クライアントとアクセスポイントで共通鍵または相手の公開鍵を予め共有しないため、認証段階において、無線通信でＩＤ情報に対して認証を行う際にも、第三者装置による盗聴、成りすましを防ぐことはできない（非特許文献１参照）。
【非特許文献１】ＩＥＥＥ　Ｓｔｄ　８０２．１１ｉ／Ｄ３．０，　Ｎｏｖｅｍｂｅｒ　２００２
【発明の開示】
【発明が解決しようとする課題】
【０００４】
以上述べたように、従来の方法では、認証用情報の共有段階において交換される認証要求と認証応答というメッセージは第三者装置（Ｍａｎ－ｉｎ－ｔｈｅ－Ｍｉｄｄｌｅ）によって盗聴・改竄される可能性がある。具体的には以下に説明する。
【０００５】
認証を行う前に、クライアントとアクセスポイントは事前、共通秘密鍵と相手の証明書をもっていないので、認証と鍵生成のために、自身の公開鍵を相手に通知することが必要となる（図２）。それを無線で送信するので、第三者によって簡単に盗聴されてしまう。
【０００６】
第三者装置は、公開鍵を取り替えることにより、クライアント側に対して、電波強度操作により、自分は本当のアクセスポイントのように、アクセスポイント側に対して自分は本当のクライアントのように装うこと（図３）を、クライアントもアクセスポイントもユーザも全然感知しない。
【０００７】
無線ＬＡＮでは、電波を伝送メディアとするので、人間にとってはそれが見えないものであり、それを利用した第三者装置は、チャンネルを変えてメッセージを転送し、送信元に転送することを隠すことができる。
【０００８】
認証の手順が破れると、鍵生成もセキュアでなくなる。
【０００９】
本発明は、前記従来の課題を解決するもので、認証用共通情報の設定を簡単化しながら、認証用情報の共有段階において第三者による盗聴となりすましを防ぐことで、認証と鍵生成をよりセキュアにする方法を提供することを目的とする。
【課題を解決するための手段】
【００１０】

前記従来の課題を解決するために、本願の請求項1における発明は、第1の通信装置と第2の通信装置との間で認証処理を行った上で前記第1の通信装置と前記第2の通信装置との間で通信を行う通信方法であって、前記第2の通信装置の公開鍵情報と、前記第2の通信装置を特定するためのＩＤ情報とを含む認証要求メッセージを前記第1の通信装置に送信する認証要求ステップと、前記第1の通信装置が受信した前記認証要求メッセージに含まれる、前記第2の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを受信した際の通信路を特定する情報とを表示する第1の表示ステップと、前記第2の通信装置が送信した前記認証要求メッセージに含まれる、前記第2の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示する第2の表示ステップと、前記第1の表示ステップと、前記第2の表示ステップで表示された前記第2の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致しているかとうかを確認する第1の確認ステップと、前記第1の確認ステップにおいて、前記第2の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第1の通信装置の公開鍵情報と、前記第1の通信装置を特定するためのＩＤ情報とを含む認証応答メッセージを前記第2の通信装置に送信する認証応答ステップと、前記第2の通信装置が受信した前記認証応答メッセージに含まれる、前記第1の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第3の表示ステップと、前記第1の通信装置が送信した前記認証応答メッセージに含まれる、前記第1の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第4の表示ステップと、前記第3の表示ステップと、前記第4の表示ステップで表示された前記第1の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致しているかとうかを確認する第2の確認ステップとで構成されることを特徴とする。

【００１１】

また、請求項2における発明は、請求項1に記載の通信方法において、前記認証要求ステップにおいて、認証要求メッセージはデジタル署名情報を更に含み、前記第1の表示ステップにおいて、前記認証要求メッセージに含まれるデジタル署名情報を復号した結果、前記第2の通信装置の署名であると確認した場合に、前記第2の通信装置を特定するためのＩＤ情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示し、前記認証応答ステップにおいて、認証応答メッセージはデジタル署名情報を更に含み、前記第3の表示ステップにおいて、前記認証応答メッセージに含まれるデジタル署名情報を復号した結果、前記第1の通信装置の署名であると確認した場合に、前記第1の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示することを特徴とする。

【００１２】

また、請求項3における発明は、請求項1または2に記載の通信方法において、前記認証要求メッセージを送信する際の通信路を特定する情報及び、前記認証応答メッセージを送信する際の通信路を特定する情報は、伝送に使用された無線チャネル情報であることを特徴とする。

【００１３】

また、請求項4における発明は、請求項1または2に記載の通信方法において、前記認証要求メッセージを送信する際の通信路を特定する情報は、前記第2の通信装置の公開鍵情報であり、前記認証応答メッセージを送信する際の通信路を特定する情報は、前記第1の通信装置の公開鍵情報であることを特徴とする。

【００１４】

また、請求項5における発明は、請求項1または2に記載の通信方法において、前記認証応答ステップにおいて、前記認証応答メッセージを前記第2の通信装置の公開鍵情報で暗号化することを特徴とする。

【００１５】
また、請求項６における発明は、請求項１または２に記載の通信方法において、前記第１の通信装置を特定するためのＩＤ情報及び前記第２の通信装置を特定するためのＩＤ情報は、通信路設定を行うたびに都度生成する乱数であることを特徴とする。
【００１６】
また、請求項７における発明は、請求項１または２に記載の通信方法において、前記第２の確認ステップにおいて、前記第１の通信装置を特定するためのＩＤ情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第２の通信装置が、自身の生成した乱数を含む共通秘密鍵生成要求メッセージを前記第１の通信装置に送信する共通秘密鍵生成要求ステップと、前記共通秘密鍵生成要求メッセージを受信した前記第１の通信装置が、自身の生成した乱数を含む共通秘密鍵生成応答メッセージを前記第２の通信装置に送信する共通秘密鍵生成応答ステップと、前記第１の通信装置が、前記共通秘密鍵生成要求メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成し、前記第２の通信装置が、前記共通秘密鍵生成応答メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成ステップを更に含むことを特徴とする。
【００１７】
また、請求項８における発明は、相手通信装置との間で認証処理を行った上で前記相手通信装置との間で通信を行う通信装置であって、自装置の公開鍵及びプライベート鍵ペアを作成する公開鍵・プライベート鍵生成手段と、前記公開鍵・プライベート鍵作成手段が生成した公開鍵情報と、自装置を識別するためのＩＤ情報とを少なくとも含む送信メッセージを生成し、前記相手通信装置に送信する送信手段と、前記相手通信装置が送信した送信メッセージを受信し、前記相手通信装置が送信した送信メッセージに含まれる前記相手通信装置の公開鍵情報と、前記相手通信装置を識別するためのＩＤ情報とを取り出す受信手段と、自装置が前記相手通信装置から送信メッセージを受信した場合、前記受信手段が取り出した前記相手通信装置を識別するためのＩＤ情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する機能と、自装置が前記相手通信装置に送信メッセージを送信した場合、自装置が送信した送信メッセージに含まれる、自装置を特定するためのＩＤ情報と、前記送信手段が送信メッセージを送信する際の通信路を特定する情報とを表示する機能とを有する表示手段と、認証を許可するかどうかを入力する入力手段とを有することを特徴とする。
【００１８】
また、請求項９における発明は、請求項８に記載の通信装置において、入力されたデータを暗号化し、その結果をデジタル署名として出力するデジタル署名手段と、前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを暗号化する暗号化手段と、前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを復号化する復号化手段と、入力されたデータに対して一方向ハッシュ関数を実行するハッシュ関数手段を更に有し、前記送信手段は、前記デジタル署名を更に含む送信メッセージを生成し、前記受信手段は、前記受信メッセージに含まれる前記相手通信装置のデジタル署名を更に取り出し、前記表示手段は、前記相手通信装置のデジタル署名を復号し、前記ハッシュ関数手段でハッシュ関数を実行してメッセージの正当性を確認できた場合に、前記受信手段が取り出した前記相手通信装置を識別するためのＩＤ情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示することを特徴とする。
【００１９】
また、請求項１０における発明は、請求項８または９に記載の通信装置において、前記通信路を特定する情報は、伝送に使用された無線チャネル情報であることを特徴とする。
【００２０】
また、請求項１１における発明は、請求項８または９に記載の通信装置において、前記

【００２１】

また、請求項１２における発明は、請求項８または９に記載の通信装置において、前記送信手段は、前記暗号化手段によって前記相手通信装置の公開鍵を使用して暗号化された送信メッセージを送信することを特徴とする。

【００２２】

また、請求項１３における発明は、請求項８または９に記載の通信装置において、乱数を発生させる擬似乱数発生手段を更に有し、前記送信手段は、前記自装置を識別するためのＩＤ情報として前記擬似乱数発生手段で生成した乱数を使用することを特徴とする。

【００２３】

また、請求項１４における発明は、請求項８または９に記載の通信装置において、入力されたデータを用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成手段を更に有し、前記共通秘密鍵生成手段は、前記相手通信装置が送信した送信メッセージに含まれる乱数を用いて、前記共通秘密鍵を生成することを特徴とする。

【発明の効果】

【００２４】

本発明によれば、第三者装置（Ｍａｎ－ｉｎ－ｔｈｅ－Ｍｉｄｄｌｅ）がクライアントとアクセスポイント間の接続設定時に交換されるメッセージへの盗聴またはなりすまし、更にクライアントやアクセスポイントに対する乗っ取りなど悪行為を防ぐことができる。

【００２５】

また、本発明によれば、認証と鍵交換を同時に行うので、クライアントとアクセスポイントで共通鍵または公開鍵の交換または事前共有することが必要でなくなる。

【００２６】

なお、本発明によれば、認証直後に、認証時に交換された公開鍵を使用して、共通秘密鍵をセキュアに生成することができる。

【００２７】

なお、本発明を他の方式の有線・無線のネットワークに適用することも可能であり、第三者攻撃を防げるという本発明の効果が得られる。

【発明を実施するための最良の形態】

【００２８】

以下本発明の実施の形態について、図面を参照しながら説明する。

【００２９】

まず、全体的な構成及び各部分の機能を説明する。図１は、認証と鍵生成のために必要とされる機能モジュール構成を示す。このモジュールは、アクセスポイント（ＡＰ）とクライアント両方ともに実装される。認証部１０は、初期化のほかに各モジュールを含め全体的にコントロールする役割を果たす。クライアントはＡＰに（初）接続されると、このモジュールが起動され、認証が開始する。それから、以後に述べる手順に基づいて、イベント処理やモジュールの呼び出しと後続処理を行う。また、認証要求メッセージの第三者装置による改竄・転送への監視とチャンネル情報表示または公開鍵表示等のコントロールも行う。認証部１０は、無線ＬＡＮカードに乗せられる。

【００３０】

公開鍵・プライベート鍵生成部１１は、自身の公開鍵・プライベート鍵ペアを生成する機能を有し、機器が起動された際に呼び出され、公開鍵・プライベート鍵を生成する。

【００３１】

デジタル署名部１２は、ハッシュ関数部１６を用いて、メッセージを固定長に短縮し、前記プライベート鍵で暗号化部１３のアルゴリズムを呼び出して暗号化し、暗号化した結果をデジタル署名として前記メッセージに付け加える。

【００３２】

暗号化部１３は、相手の公開鍵または自身のプライベート鍵または相手と共有する共通秘密鍵を用いて暗号化するためのアルゴリズムを含む。

【００３３】

復号部１４は、相手の公開鍵または自身のプライベート鍵または相手と共有する共通秘密鍵を用いて復号するためのアルゴリズムを含む。

【００３４】

擬似乱数発生部１５は、規則性を予測しにくい擬似乱数生成機能を有し、ノンスや（必要な時）ＩＤを生成するためのモジュールである。

【００３５】

ハッシュ関数部１６は、長いビット列を固定長のビット列に圧縮する一方向ハッシュ関数を含む。

【００３６】

共通秘密鍵生成部１７は、二つのノンス（乱数）に基づき、擬似乱数発生部１５を用いて秘密鍵を生成するモジュールである。

【００３７】

送信部１８は、認証部１０から必要な情報を取得し、送信メッセージを組み立てると共に、ＭＡＣレイヤでメッセージの送信をコントロールし、送信に使用されたチャンネルの情報（例えば、チャンネル番号）を前記認証部１０に返す。また、自機器を特定するためのＩＤ情報（例えば、機器に設定された名前やＭＡＣアドレス）を保持する。

【００３８】

受信部１９は、ＭＡＣレイヤでメッセージの受信をコントロールし、受信メッセージから必要な情報を取り出して認証部１０に渡す。また、受信に使用されたチャンネルの情報（例えば、チャンネル番号）を前記認証部１０に返す。

【００３９】

表示部２０は、送受信に伴って、ＩＤ情報とチャンネル情報または公開鍵を表示する装置であって、ユーザに確認して認証許可判断を行なわせる。

【００４０】

入力部２１は、ユーザの認証許可判断を入力させるために備えた装置（例えば、ボタン）である。

【００４１】

前記公開鍵・プライベート鍵生成部１１、デジタル署名部１２、暗号化部１３、復号部１４、擬似乱数発生部１５、ハッシュ関数部１６、共通秘密鍵生成部１７は、図１のように認証部の内部モジュールとして認証部と一体になって実装してもよいし、個別的に認証部の外に置いてまたは使用可能な外部共通モジュールを呼び出して使用するという形での実装でもよい。

【００４２】

次に、認証と鍵生成に関する手順の実施について説明する。

【００４３】

（実施の形態１）

図４に、クライアント２をＡＰ１に接続する際に、本発明による接続の手順を示す。プローブ要求３００は、従来標準のフォーマットを採用する。プローブ応答３０１は、従来のプローブ応答のサポートできる接続方式リストに本発明の接続方式を追加したフォーマットを採用する。プローブ確認３０２は、従来標準にはなく、本発明の接続方式を行うこととそれに必要なパラメータを知らせる機能を持つ新しいメッセージタイプである。認証要求３０３以降のメッセージは全て本発明規定の新しいフォーマットを採用する。認証要求３０３のフォーマットを図５に示す。ＨＤＲｃ　１００１はクライアント２のアドレスやメッセージタイプを含むヘッダーであり、従来の認証要求のヘッダーと同様である。ＰＬｃ　１００２は従来と同じようなペイロードである。ＰＫｃ　１００３は前記クライアント２の公開鍵である。ＩＤｃ　１００４は前記クライアント２のＩＤである。ＳＩＧＮｃ　１００５は、ヘッダーをはじめ全てのフィールドに対して前記クライアント２のデジ

ル署名部１２を用いて署名したものである。クライアント２の送信部１８は、公開鍵・プライベート鍵生成部１１からクライアント２の公開鍵ＰＫｃ　１００３を取得する。また、デジタル署名部１２からＳＩＧＮｃ　１００５を取得し、送信部１８が保持するＩＤｃ　１００４と合わせて認証要求３０３を生成する。認証要求３０３によって、クライアント２の公開鍵ＰＫｃをＡＰ１に渡すことが出来る。

【００４４】

クライアント２が認証要求３０３を送信し、クライアント２自身の表示部２０に、ＩＤｃと自身の送信部１８で送信に使用されたチャンネルの情報（例えば、無線チャンネル番号）を表示する。

【００４５】

ＡＰ１が認証要求３０３を受信すると、ＡＰ１の受信部１９は認証要求３０３に含まれるクライアント２の公開鍵ＰＫｃ　１００３と、デジタル署名ＳＩＧＮｃ　１００５を取り出し、ＡＰ１の認証部１０に渡す。クライアント２の公開鍵ＰＫｃ　１００３とＡＰ１自身の復号部１４を用いてＳＩＧＮｃ　１００５を復号した結果を、受信した認証要求３０３に対し、ＡＰ１のハッシュ関数部１６で自身のハッシュ関数を用いて、クライアント２の署名時に使用した同じハッシュ関数を掛けた結果と比較し（即ち、完全性チェックを行い）、一致したら、受信した認証要求３０３に含まれたＩＤと、ＡＰ１の受信部１９で受信に使用されたチャンネルの情報（例えば、無線チャンネル番号）をＡＰ１自身の表示部２０に表示する。ユーザが、クライアント２の表示部２０に表示されているＩＤ及びチャンネル情報と、ＡＰ１の表示部２０に表示されているＩＤ及びチャンネル情報とが一致するかしないかを確認し、一致したら、認証許可をＡＰ１の入力部２１を用いて行う。

【００４６】

なお、本実施の形態では、デジタル署名ＳＩＧＮｃを復号し、完全性を確認できた場合に、受信した認証要求に含まれたＩＤと、受信部で受信に使用されたチャンネルの情報をＡＰ１自身の表示部２０に表示しているが、デジタル署名を使用せず、受信した認証要求の内容を無条件に表示し、一致を確認しても良い。

【００４７】

前記認証要求を行う際に、図３のように第三者装置３が入り込んでしまうと、クライアント２から送信された認証要求は、第三者装置３に盗聴されて、そのまま転送されるか、または、第三者装置３が受信した認証要求３０３に対して、図８に示すように、公開鍵ＰＫｃ　１００３を自身の公開鍵ＰＫｍ　１３０３に取り替えて、また、署名ＳＩＧＮｃ　１００５も自身のプライベート鍵による署名ＳＩＧＮｍ　１３０５に取り替えて、こうして改竄した認証要求４０２をＡＰ１へ送出するかということがあるが、何れクライアント２またはＡＰ１の監視によって検知される。検知された結果を表示部に表示し、認証中断とする。第三者装置３が傍受しているだけの場合は、理解できるのは暗号化していない前記認証要求または後の認証応答だけであり、それ以降にやりとりされるメッセージは、交換した公開鍵ＰＫｃ及びＰＫａで暗号化される。このため、認証に対して悪影響をもたらそうとするのはこの認証方法により不可能である。また、第三者装置３が、クライアント２の送信に使用された送信チャンネルを異なったチャンネルで転送した場合は、前記クライアント２とＡＰ１の表示部に表示されたチャンネル情報の一致性確認によって検知される。

【００４８】

前記認証要求が成功した場合、ＡＰ１からクライアント２へ認証応答３０５を返信する。認証応答３０５のフォーマットを図６に示す。ＰＬａ　１１０２は認証結果を含む。ＰＫａ　１１０３はＡＰ１の公開鍵である。ＩＤａ　１１０４はＡＰ１のＩＤである。ＳＩＧＮａ　１１０５は、ＡＰ１のプライベート鍵とデジタル署名部を用いて認証応答３０５の各フィールドに対する署名である。ＡＰ１の送信部１８は、公開鍵・プライベート鍵生成部１１からクライアント１の公開鍵ＰＫａ　１１０３を取得する。また、デジタル署名部１２からＳＩＧＮａ　１１０５を取得し、送信部１８が保持するＩＤａ　１１０４と合わせて認証応答３０５を生成する。認証応答３０５によって、ＡＰ１の公開鍵ＰＫａをク

クライアント２に渡すことが出来る。

【００４９】

ＡＰ１が認証応答３０５を送信した後、ＡＰ１自身の送信部１８で送信に使用されたチャンネルの情報（例えば、無線チャンネル番号）とＩＤａをＡＰ１自身の表示部２０に表示し、認証応答３０５を第三者装置に改竄・転送されるのを監視する。

【００５０】

クライアント２が認証応答３０５を受信すると、クライアント２の受信部１９は、認証応答３０５に含まれるＡＰ１の公開鍵ＰＫａ　１１０３と、デジタル署名ＳＩＧＮａ　１１０５を取り出し、クライアント２の認証部１０に渡す。そして、ＡＰ１と同様の方法でメッセージの完全性をチェックする。完全性に問題がなければ、受信した認証応答３０５に含まれたＩＤと、クライアントの受信部１９で受信に使用されたチャンネルの情報（例えば、チャンネル番号）をクライアント２自身の表示部２０に表示する。ユーザが、クライアント２の表示部２０とＡＰ１の表示部２０とに表示されているＩＤとチャンネル情報とをそれぞれ確認し、一致したら、認証許可をクライアント２の入力部２１を用いて行い、認証成功となる。

【００５１】

（実施の形態２）

認証要求メッセージが第三者装置に改竄・転送されることに対する監視を、クライアント２またはＡＰ１が行う。クライアント２が行うのが、第三者装置の送信したメッセージ全てをクライアント２が受信できる状況にある場合に有効である。ＡＰ１が行うのが、クライアント２の送信したメッセージと第三者装置の送信したメッセージ全てをＡＰ１が受信できる状況にある場合に有効である。クライアント２が行う場合は、ＡＰ１からの認証応答が返信されるまでに受信した第三者装置の改竄した認証要求は、含まれた公開鍵と署名を除いて自身の送出した認証要求と同じであれば、第三者装置の改竄・転送行為を断定する。ＡＰ１が行う場合は、一定時間内に公開鍵と署名を除いて全く同じ認証要求を二つ受信すれば、第三者装置の改竄・転送行為を断定する。ＡＰ１が図８に示すような認証応答４０２を受信したら、公開鍵ＰＫｍ　１３０３と署名ＳＩＧＮｍ　１３０５を除いて同じ認証応答を二つ受信しているか、クライアント２も自身が送信した認証要求の公開鍵と署名を改竄されたこの認証要求を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

【００５２】

認証応答メッセージが第三者装置に改竄・転送されることに対する監視・断定は、前記認証要求メッセージと同じような処理の仕方を用い、クライアント２とＡＰ１と役割を交換すればよい。クライアント２が図９に示すような認証応答４０４を受信したら、公開鍵ＰＫｍ　１４０３と署名ＳＩＧＮｍ　１４０５を除いて同じ認証応答を二つ受信しているか、ＡＰ１も自身が送信した認証応答の公開鍵と署名を改竄されたこの認証応答を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

【００５３】

（実施の形態３）

認証要求メッセージまたは認証応答メッセージを第三者装置に改竄・転送されることを断定するために、監視とチャンネル情報表示という手法を使用するのではなく、認証要求メッセージまたは認証応答メッセージに含まれる公開鍵を表示して、クライアント２の表示部２０とＡＰ１の表示部２０に表示された公開鍵の一致性をユーザに確認させ、認証許可を行わせる。

【００５４】

公開鍵は長いので、表示部に一遍で表示し切れない場合は、ハッシュ関数部１６を用いて短縮して表示するか、図示しないスイッチを設けて表示部２０と連動させ、スライドで表示させてもよい。

【００５５】

（実施の形態４）

認証応答３０５は図７に示すようなフォーマットを採用する。ＡＰ１の暗号化部１３が、認証応答情報ＰＬａ　１２０２、ＡＰ１の公開鍵ＰＫａ　１２０３、ＡＰ１のＩＤａ　１２０４を、認証要求３０３で受け取ったクライアント２の公開鍵ＰＫｃで暗号化して、認証応答３０５をクライアント２に送信する。このような認証応答３０５は、公開鍵ＰＫｃのペアであるプライベート鍵をもつクライアント２しか復号できない。なお、このような認証応答３０５を使用した場合は、ＩＤとチャンネル情報または公開鍵ＰＫｃの表示と確認を行う必要がなくなる。

【００５６】

なお、この場合は、認証要求を行う段階で第三者装置の改竄はないと確認できたので、クライアント２またはＡＰ１が図１０に示すような認証応答４０４を受信することはない。第三者装置がこの段階からこのような認証応答を使用して攻撃しても、クライアント２にただ無視され、悪影響にはならない。

【００５７】

（実施の形態５）

クライアント２またはＡＰ１のＩＤとして、クライアントの接続を行う都度にクライアント２及びＡＰ１の擬似乱数発生部１５で生成した乱数を使用する。これは、ＭＡＣアドレスや製品の型番より、より高い秘密性を持つ。ユーザ定義の名前をＩＤとしてここで使うことも可能であるが、事前、入力しておく手間がかかり、且つ、ユーザはなるべくユニーク（特に隣家の同様な機器と異なるよう）な名前を設定しなければならない。乱数を使用することで、次回接続時には、違うＩＤになるので、盗まれても問題はない。

【００５８】

（実施の形態６）

認証に成功した場合、クライアント２は、ＡＰ１へ図１１に示すような共通秘密鍵生成要求３０７を送信する。共通秘密鍵生成要求３０７は、ヘッダーＨＤＲｃ　１６０１を除いた部分がクライアント２の暗号化部１３においてＡＰ１の公開鍵ＰＫａを用いて暗号化される。ＩＤｃ　１６０２はクライアント２のＩＤである。Ｎｃ　１６０３はクライアント２が生成したノンス（乱数）である。クライアント２の暗号化部１３は、クライアント２の送信部１８が保持するＩＤｃと、クライアント２の擬似乱数発生部１５が生成したノンス（乱数）Ｎｃを取得し、暗号化する。クライアント２の送信部１８は、暗号化されたＩＤｃと、ノンス（乱数）ＮｃにヘッダーＨＤＲｃ　１６０１を付加し、共通秘密鍵生成要求３０７を送信する。ＡＰ１の受信部１９が、共通秘密鍵生成要求３０７を受信し、復号の対象となるデータを取り出して復号部１４に渡す。復号部１４において、自身のプライベート鍵で復号する。復号結果において、ＩＤは先に認証したクライアント２のＩＤｃであることを確認する。確認できたら、復号結果で得られたＮｃを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通秘密鍵生成要求３０７を廃棄し、鍵生成を中止とする。

【００５９】

ＡＰ１が、共通秘密鍵生成要求３０７を正確に受信し且つ確認できた場合には、クライアント２に、図１２に示すような共通秘密鍵生成応答３０８を返信する。共通秘密鍵生成応答３０８は、ヘッダーＨＤＲａ　１７０１を除いた部分がクライアント２の公開鍵ＰＫｃを用いて暗号化される。ＩＤａ　１７０２はＡＰ１のＩＤである。Ｎａ　１７０３はＡＰ１が生成したノンス（乱数）である。ＡＰ１の暗号化部１３は、ＡＰ１の送信部１８が保持するＩＤａと、ＡＰ１の擬似乱数発生部１５が生成したノンス（乱数）Ｎａを取得し、暗号化する。ＡＰ１の送信部１８は、暗号化されたＩＤａと、ノンス（乱数）ＮａにヘッダーＨＤＲａ　１７０１を付加し、共通秘密鍵生成応答３０８を送信する。クライアント２の受信部１９が、共通秘密鍵生成応答３０８を受信し、復号の対象となるデータを取り出して復号部１４に渡す。復号部１４において、自身のプライベート鍵で復号する。復号結果において、ＩＤは先に認証したＡＰ１のＩＤａであることを確認する。確認できたら、復号結果で得られたＮａを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通秘密鍵生成応答３０８を廃棄し、鍵生成を中止とする。

【００６０】
鍵生成は、ＡＰ１及びクライアント２の共通秘密鍵生成部１７において、ＮｃとＮａ及び次の式に基づいて行う。鍵　＝　ｐｒｆ（ＰｒｅＭａｓｔｅｒＫｅｙ，“ｃｏｎｔｒｏｌ”　||　ＩＤＡＤＤＲｃ　||　ＩＤＡＤＤＲａ　||　Ｎｃ　||　Ｎａ）。但し、ｐｒｆ　は擬似乱数関数である。ＰｒｅＭａｓｔｅｒＫｅｙはこの発明の実施にあたって内部で設定した共通な数値である。ＩＤＡＤＤＲｃはクライアント２のＩＤまたはＭＡＣアドレス、ＩＤＡＤＤＲａ　はＡＰ１のＩＤまたはＭＡＣアドレスである。ＮｃとＮａは、前記認証時に交換されたクライアントとＡＰのノンスである。これで、ＡＰ１とクライアント２は、同じ鍵を生成し、共有することになる。

【００６１】
クライアント２とＡＰ１が生成した前記共通秘密鍵を、次のアソシエーションの作成に用いる。つまり、図４のアソシエーション要求３０９もアソシエーション応答３１０も、この鍵を用いて暗号化される。一方、受信側は、この鍵を用いて受信したメッセージを復号する。

【００６２】
前記生成した鍵は、クライアント２とＡＰ１間のコントロールメッセージの送受信に用いるが、データ送受信のために別の鍵を用いてもよい。その場合は、鍵　＝　ｐｒｆ（ＰｒｅＭａｓｔｅｒＫｅｙ，“ｄａｔａ”　||　ＩＤＡＤＤＲｃ　||　ＩＤＡＤＤＲａ　||　Ｎｃ　||　Ｎａ）　という式を用いて生成する。

【００６３】
以上の文章と図の中には、クライアントとアクセスポイントとの間の認証と鍵生成に関するアーキテクチャのみ記述した。しかし、実際には、アクセスポイントの向こうがルータ或いはホームゲートウェイの場合は、アクセスポイントをルータ或いはホームゲートウェイに代わってクライアントとの認証・鍵生成を行ってもよい。つまり、クライアントの認証と鍵生成の相手は、ルータあるいはホームゲートウェイになる。但し、この場合には、ルータ或いはホームゲートウェイは、アクセスポイントとセキュアな通信経路で繋がれており、アクセスポイントは中継機能を果たす。なお、本発明は、ルータ或いはホームゲートウェイとアクセスポイントとの間に無線ＬＡＮで繋ぐ場合の接続にも応用できる。

【産業上の利用可能性】

【００６４】
本発明の提案したセキュリティ強度を高めた接続方法は、第三者（Ｍａｎ－ｉｎ－ｔｈｅ－Ｍｉｄｄｌｅ）攻撃を予防・排除できる特徴を有し、無線ＬＡＮの目視認証及び鍵生成をよりセキュアにする方法として有用である。また、第三者攻撃が存在しうる他のタイプの有線・無線ネットワークにおける相互認証と鍵生成にも応用できる。

【図面の簡単な説明】

【００６５】
【図１】本発明の機能モジュール構成図
【図２】従来の無線ＬＡＮにおける目視認証の接続処理の流れ図
【図３】第三者装置（Ｍａｎ－ｉｎ－ｔｈｅ－Ｍｉｄｄｌｅ）が侵入した場合の状況図
【図４】本発明の接続処理の流れ図
【図５】本発明の認証要求メッセージのフォーマット図
【図６】本発明の認証応答メッセージのフォーマット図（案１）
【図７】本発明の認証応答メッセージのフォーマット図（案２）
【図８】第三者装置によって改竄・転送された認証要求メッセージのフォーマット図
【図９】第三者装置によって改竄・転送された認証応答メッセージのフォーマット図（案１）
【図１０】第三者装置によって改竄・転送された認証応答メッセージのフォーマット図（案２）
【図１１】本発明の共通秘密鍵生成要求メッセージのフォーマット図

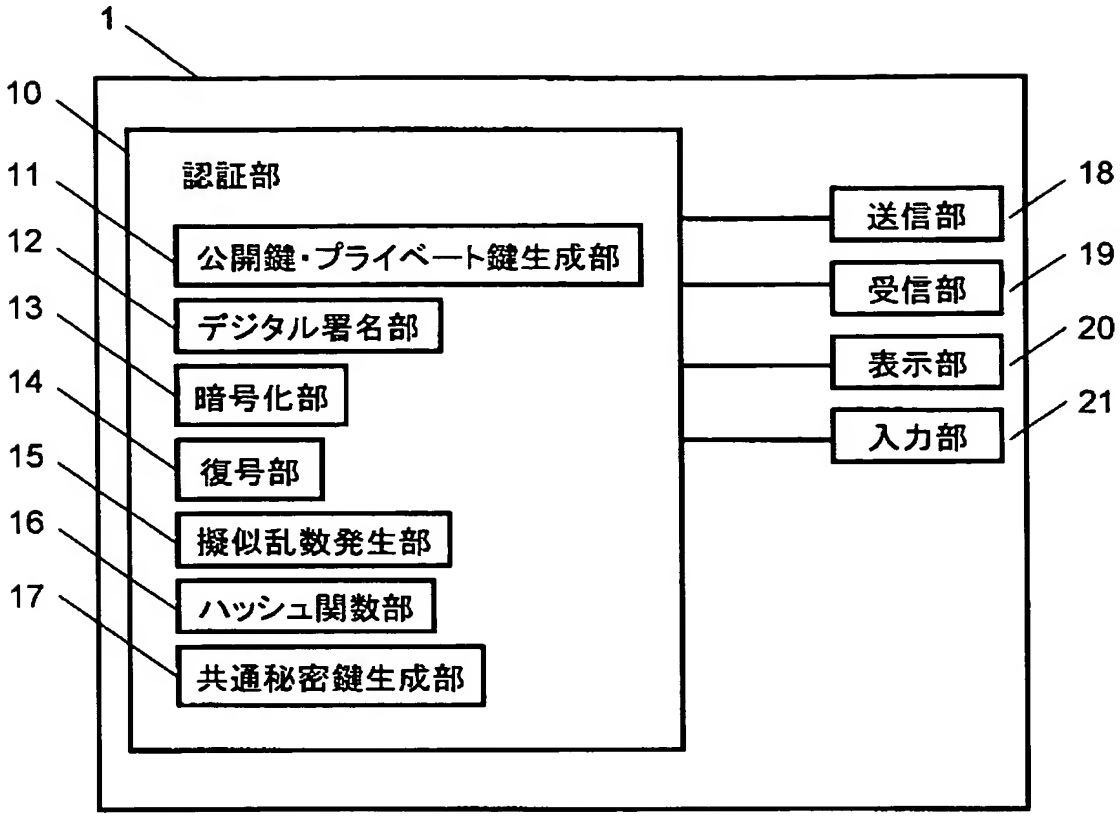
【図１２】本発明の共通秘密鍵生成応答メッセージのフォーマット図

【符号の説明】

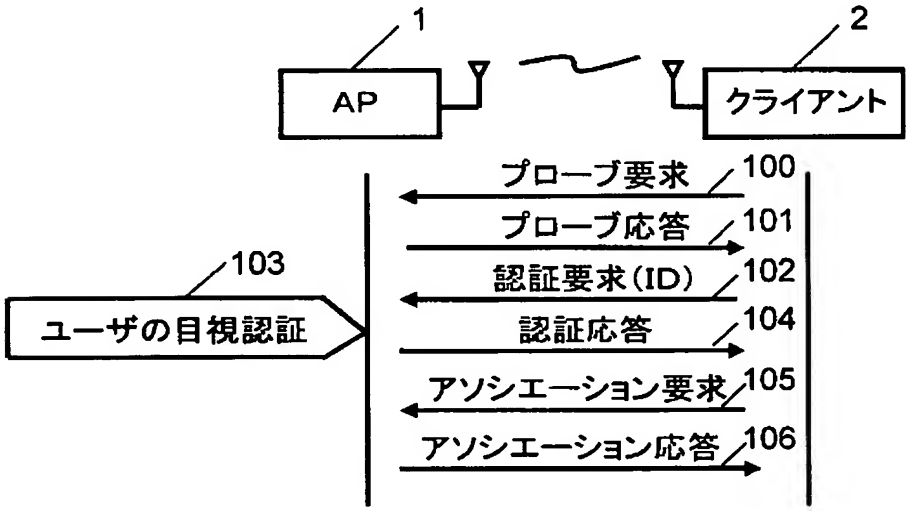
【００６６】

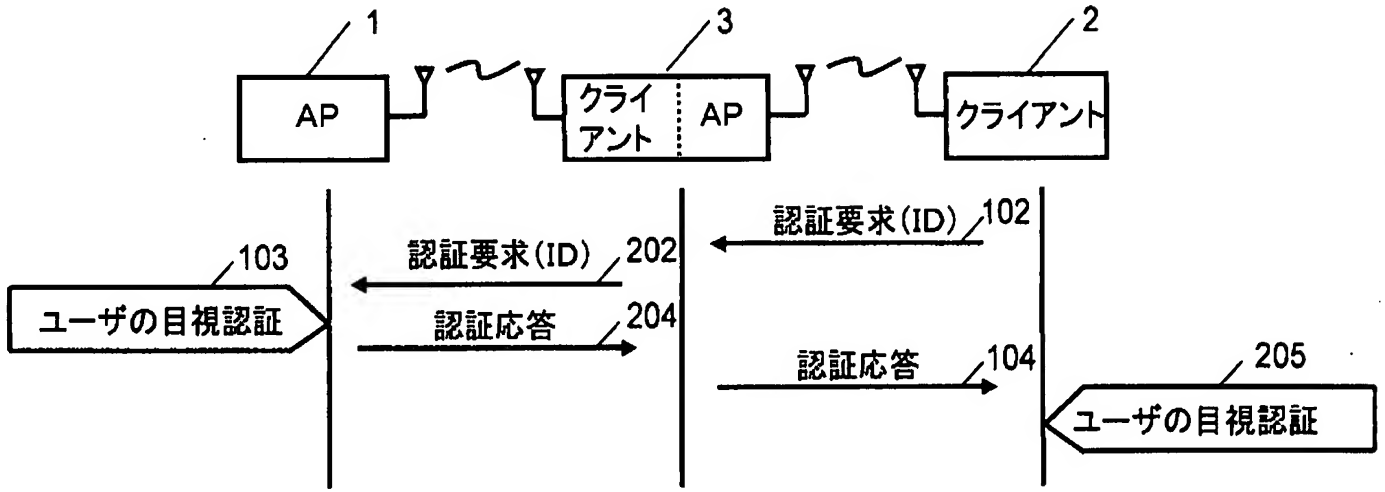
１　認証・鍵生成機能ブロック
１０　認証部
１１　公開鍵・プライベート鍵生成部
１２　デジタル署名部
１３　暗号化部
１４　復号部
１５　擬似乱数発生部
１６　ハッシュ関数部
１７　共通秘密鍵生成部
１８　送信部
１９　受信部
２０　表示部
２１　入力部

【書類名】図面
【図１】

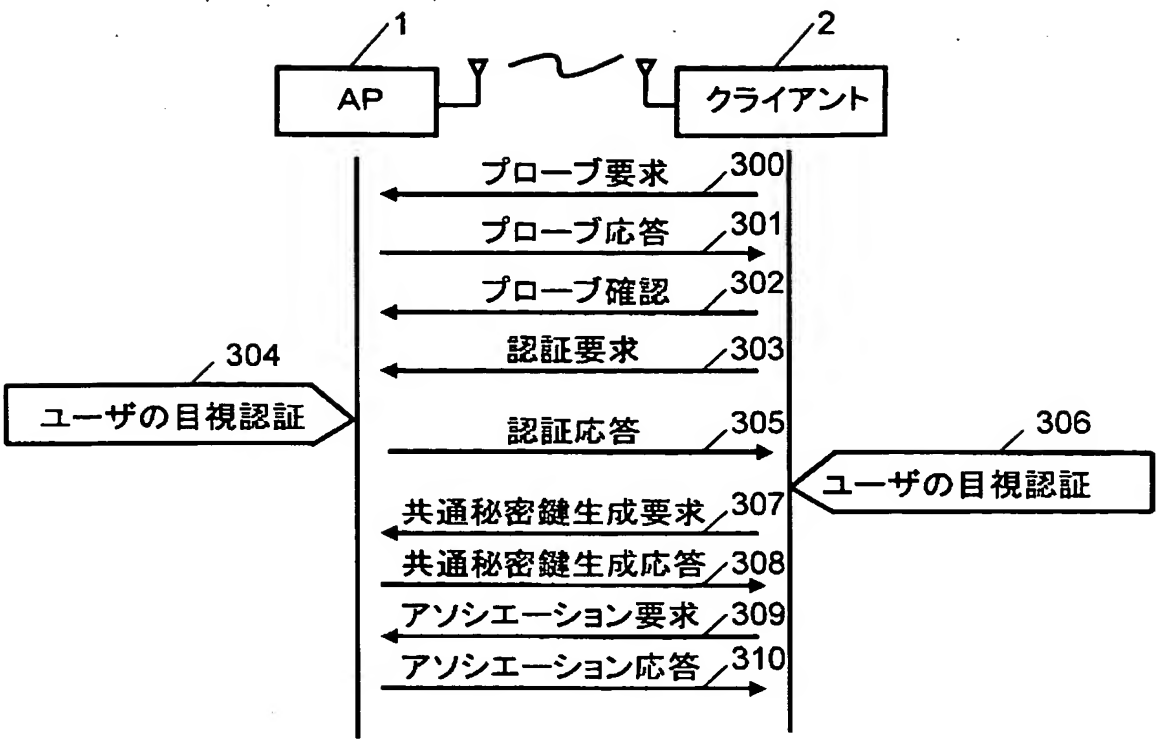

1
10
認証部
11
公開鍵・プライベート鍵生成部
12
デジタル署名部
13
暗号化部
14
復号部
15
擬似乱数発生部
16
ハッシュ関数部
17
共通秘密鍵生成部
送信部
18
受信部
19
表示部
20
入力部
21

【図２】

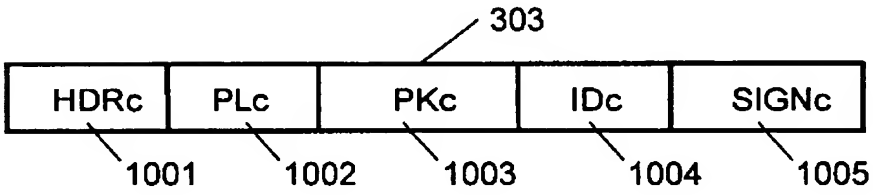

1
AP
2
クライアント
プローブ要求
100
プローブ応答
101
認証要求(ID)
102
認証応答
104
アソシエーション要求
105
アソシエーション応答
106
103
ユーザの目視認証


1
3
2
AP
クライアント
AP
クライアント
認証要求(ID)
102
103
認証要求(ID)
202
ユーザの目視認証
認証応答
204
認証応答
104
205
ユーザの目視認証

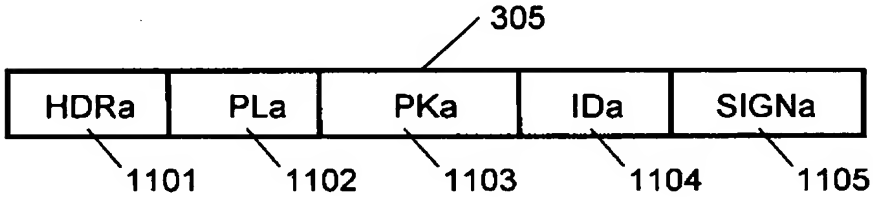
【図４】


1
2
AP
クライアント
プローブ要求
300
プローブ応答
301
プローブ確認
302
認証要求
303
304
ユーザの目視認証
認証応答
305
306
ユーザの目視認証
共通秘密鍵生成要求
307
共通秘密鍵生成応答
308
アソシエーション要求
309
アソシエーション応答
310

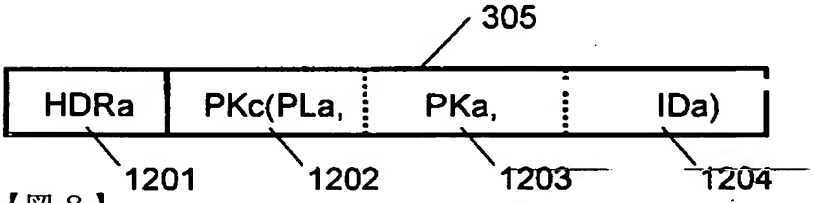
【図５】


303
HDRc
PLc
PKc
IDc
SIGNc
1001
1002
1003
1004
1005

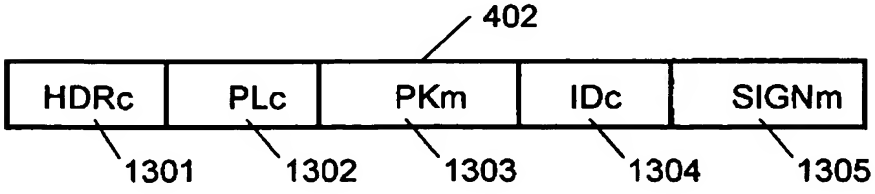
【図６】


305
HDRa
PLa
PKa
IDa
SIGNa
1101
1102
1103
1104
1105

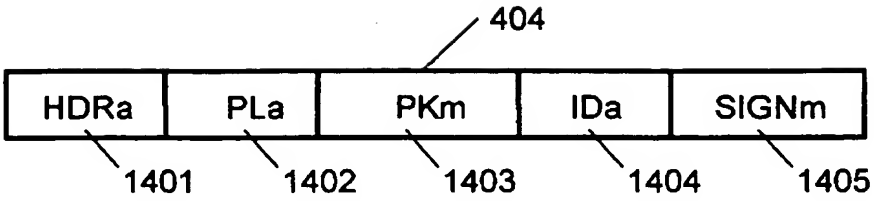
【図７】


305
HDRa
PKc(PLa,
PKa,
IDa)
1201
1202
1203
1204

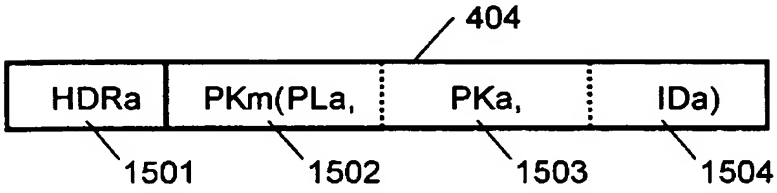
【図８】


402
HDRc
PLc
PKm
IDc
SIGNm
1301
1302
1303
1304
1305

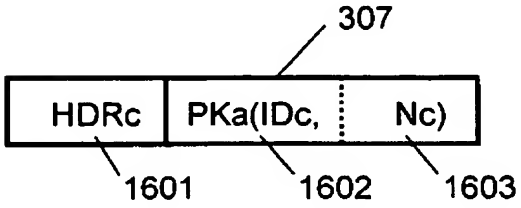
【図９】



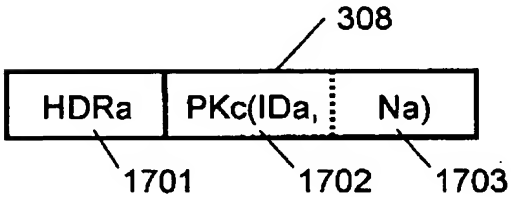
【図１０】



【図１１】



【図１２】



【書類名】要約書

【要約】

【課題】無線ＬＡＮの接続において、共通鍵や証明書を利用しない場合、ユーザは目視で認証するという簡単な方法を用いる際に、第三者（Ｍａｎ－ｉｎ－ｔｈｅ－Ｍｉｄｄｌｅ）による盗聴となりすまし等悪行為を防ぐこと。

【解決手段】公開鍵・プライベート鍵生成部１１と、デジタル署名部１２と、暗号化部１３と、復号部１４と、擬似乱数発生部１５と、ハッシュ関数部１６と、共通秘密鍵生成部１７とを備え、認証要求メッセージと認証応答メッセージに公開鍵とＩＤを加えて、プライベート鍵で署名して、または、公開鍵で暗号化して送信する。受信側は復号して、含まれた情報を表示部２０に表示する。ユーザはクライアントとＡＰ間の表示部に表示された情報の一致性を確認して入力部２１を通して認証を行う。こうすることにより、第三者装置の盗聴となりすましを防ぎ、両通信装置間の認証と鍵生成はセキュアとなる。

【選択図】図１

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007096

International filing date: 12 April 2005 (12.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-147422
Filing date: 18 May 2004 (18.05.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse